UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,490	07/07/2003	Nicolas Cerf	VANM256.001AUS	8981

20995 7590 01/30/2006

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER
LOVING, JARIC E

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/615,490	CERF ET AL.	
	Examiner	Art Unit	
	Jaric Loving	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 July 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *12/15/03, 2/27/04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

From pages 2-23, there are numerous instances of words containing superscripts with no corresponding references for them.

On pages 15-17, Figure 1 is discussed along with its corresponding components, but no reference numerals from the drawings are cited.

Appropriate correction is required.

2. Claims 1 and 12 are objected to because of the following informalities: In claim 1, line 2, the phrase "at least one sending unit comprising and encoder..." should be --at least one sending unit comprising an encoder--. In claim 12, line 2, the phrase "coherent sates..." should be --coherent states--. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Nambu, US 6,801,626.

In claim 1, Nambu discloses a quantum cryptographic system comprising:

at least one sending unit comprising and encoder and distributing a raw key in the quadrature components of quantum coherent states that are continuously modulated in phase and amplitude (abstract; col. 1, lines 14-48; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 44);

at least one receiving unit comprising a homodyne detector of the quantum coherent states in order to measure the quadrature components of the states (abstract; col. 1, lines 14-48; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53);

a quantum channel for connecting the sending unit to the receiving unit (col. 1, lines 14-48); and

a two-way authenticated public channel for transmitting non-secret messages between the sending unit and the receiving unit (col. 1, lines 14-48; col. 4, line 63 – col. 5, line 53).

In claim 2, Nambu discloses the quantum cryptographic system of claim 1, further comprising a continuous-variable quantum key distribution protocol ensuring that the amount of information a potential eavesdropper may gain at most on the sent and received data can be estimated from the measured parameters of the quantum channel (error rate and line attenuation) (col. 1, lines 14-48; col. 4, lines 4-42; col. 4, line 63 – col. 5, line 53).

In claim 3, Nambu discloses the quantum cryptographic system of claim 2, wherein the sent and received raw data resulting from the continuous-variable protocol are converted into a secret binary key by using a continuous reconciliation protocol supplemented with privacy amplification (col. 1, lines 14-48; col. 2, lines 32-57; col. 4, lines 4-42; col. 4, line 63 – col. 5, line 53).

In claim 4, Nambu discloses the quantum cryptographic system of claim 1, wherein the encoder of the quadrature components with a high signal-to-noise ratio encodes several key bits per coherent light pulse (col. 4, lines 4-42; col. 4, line 63 – col. 5, line 53).

In claim 5, Nambu discloses the quantum cryptographic system of claim 1, wherein the decoding of the quadrature components of the light field via the homodyne detector achieves high secret bit rates in comparison to photon-counting techniques (col. 4, line 63 – col. 5, line 53).

In claim 6, Nambu discloses the quantum cryptographic system of claim 3, wherein the continuous reconciliation protocol is a direct reconciliation protocol, which allows the receiver to discretize and correct its data according to the sent values, in case of noisy quantum channels with low losses (col. 1, lines 14-48; col. 4, lines 4-42; col. 2, lines 32-57).

In claim 7, Nambu discloses the quantum cryptographic system of claim 3, wherein the continuous reconciliation protocol is a reverse reconciliation protocol, which allows the sending unit to discretize and correct its data according to the values measured by the receiver, in case of quantum channels with an attenuation that exceeds 3 dB (col. 1, lines 14-48; col. 4, lines 4-42; col. 2,.lines 32-57).

In claim 8, Nambu discloses the quantum cryptographic system of claim 3, wherein the secret key is used as a private key for ensuring confidentiality and authentication of a cryptographic transmission (col. 2, lines 32-57).

In claim 9, Nambu discloses the quantum cryptographic system of claim 1, wherein the quadrature components of the quantum coherent states are modulated with a Gaussian distribution (col. 9, line 60 – col. 11, line 12).

In claim 10, Nambu discloses the quantum cryptographic system of claim 9, wherein the co-ordinate values of the center of the Gaussian distribution are arbitrary (col. 9, line 60 – col. 11, line 12).

In claim 11, Nambu discloses the quantum cryptographic system of claim 9, wherein the variance of the Gaussian distribution for the quadrature X is different from the variance of the Gaussian distribution for the conjugate quadrature P (col. 9, line 60 – col. 11, line 12).

In claim 12, Nambu discloses the quantum cryptographic system of claim 9, wherein the Gaussian-modulated coherent sates are attenuated laser light pulses typically containing several photons (abstract; col. 4, line 63 – col. 5, line 53; col. 9, line 60 – col. 11, line 12).

In claim 13, Nambu discloses the quantum cryptographic system of claim 12, wherein the information an eavesdropper may gain on the sent and received Gaussian-distributed values are calculated explicitly using Shannon's theory for Gaussian channels (col. 2, line 32-57; col. 6, line 34 – col. 7, line 6; col. 9, line 60 – col. 11, line 12).

In claim 14, Nambu discloses a method of distributing continuous quantum key between two parties which are a sender and a receiver, the method comprising:

selecting, at a sender, two random numbers x_A and p_A from a Gaussian distribution of mean zero and variance V_AN_0, where N_0 refers to the shot-noise variance (col. 9, line 60 – col. 11, line 12);

sending a corresponding coherent state $|x_A + ip_A >$ in the quantum channel (col. 4, line 63 – col. 5, line 53);

randomly choosing, at a receiver, to measure either quadrature x or p using homodyne detection (col. 4, line 63 – col. 5, line 53; col. 6, line 34 – col. 7, line 6; col. 9, lines 36-59);

informing the sender about the quadrature that was measured so the sender may discard the wrong one (col. 2, lines 32-57);

measuring channel parameters on a random subset of the sender's and receiver's data, in order to evaluate the maximum information acquired by an eavesdropper (col. 2, lines 32-57; col. 4, lines 4-42); and

converting the resulting raw key in the form of a set of correlated Gaussian variables into a binary secret key comprising direct or reverse reconciliation in order to correct the errors and get a binary key, and privacy amplification in order to make secret the binary key (col. 2, lines 32-57; col. 4, lines 4-42; col. 9, line 60 – col. 11, line 12).

In claim 15, Nambu discloses the method of claim 14, wherein the reconciliation produces a common bit string from correlated continuous data, which comprises the following:

transforming each Gaussian key element of a block of size n by the sender into a string of m bits, giving m bit strings of length n, referred to as slices (col. 4, line 63 – col. 5, line 53; col. 9, line 60 – col. 11, line 12);

converting, by the receiver, the measured key elements into binary strings by using a set of slice estimators (col. 4, line 63 – col. 5, line 53; col. 9, lines 36-59); and

sequentially reconciliating the slices by using an implementation of a binary error correction algorithm, and communicating on the public authenticated channel (col. 2, lines 32-57; col. 7, lines 7-14).

In claim 16, Nambu discloses the method of claim 14, wherein the post-processing of privacy amplification comprises distilling a secret key out of the reconciliated key by use of a random transformation taken in a universal class of hash functions (col. 2, lines 32-57; col. 4, lines 4-42).

In claim 17, Nambu discloses a device for implementing a continuous-variable quantum key exchange, the device comprising:

a light source or a source of electromagnetic signals configured to generate short quantum coherent pulses at a high repetition rate (col. 4, line 63 – col. 5, line 53);

an optical component configured to modulate the amplitude and phase of the pulses at a high frequency (col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53);

a quantum channel configured to transmit the pulses from an emitter to a receiver (col. 4, line 63 – col. 5, line 53);

a system that permits the transmission of a local oscillator from the emitter to the receiver (col. 4, line 63 – col. 5, line 53; col. 7, lines 7-49);

a homodyne detector capable of measuring, at a high acquisition frequency, any quadrature component of the electromagnetic field collected at the receiver's station (col. 4, line 63 – col. 5, line 53);

a two-way authenticated public channel that is used to communicating non-secret messages in postprocessing protocols (col. 1, lines 14-48; col. 4, line 63 – col. 5, line 53); and

a computer at the emitter's and receiver's stations that drives or reads the optical components and runs the postprocessing protocols (col. 4, line 63 – col. 5, line 53; col. 8, line 39 – col. 9, line 59).

In claim 18, Nambu discloses the device of claim 17, wherein a local oscillator is transmitted together with the signal by use of a polarization encoding system whereby each pulse comprises a strong local oscillator pulse and a weak orthogonally-polarized signal pulse with modulated amplitude and phase (col. 2, lines 10-31; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53).

In claim 19, Nambu discloses the device of claim 18, wherein if polarization encoding is used, the receiving system relies on polarization-mode homodyne detection requiring a quarter-wave plate and a polarizing beam splitter (col. 2, lines 10-31; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53).

In claim 20, Nambu discloses the device for exchanging Gaussian key elements between two parties which are a sender and a receiver, the device comprising:

a laser diode associated with a grating-extended external cavity, the laser diode configured to send light pulses at a high repetition rate, each pulse typically containing several photons (col. 4, line 63 – col. 5, line 53; col. 7, lines 7-28);

an integrated electro-optic amplitude modulator and a piezoelectric phase modulator, configured to generate randomly-modulated light pulses, the data being organized in bursts of pulses (col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53; col. 7, lines 7-28);

a beam-splitter to separate the quantum signal from a local oscillator (col. 8, line 39 – col. 9, line 22); and

a homodyne detector combining the quantum signal and local oscillator pulses in order to measure one of the two quadrature components of the light field (col. 8, line 39 – col. 9, line 22).

In claim 21, Nambu discloses the device of claim 20, further comprising an acquisition board and a computer on the sender's and receiver's sides in order to run the post-processing protocols (col. 4, line 63 – col. 5, line 53; col. 8, line 39 – col. 9, line 59).

In claim 22, Nambu discloses the device of claim 20, wherein the laser operates at a wavelength comprised between about 700 and about 1600 nm (col. 7, lines 7-28).

In claim 23, Nambu discloses the device of claim 20, wherein the laser operates at a wavelength comprising telecom wavelengths between about 1540 and about 1580 nm (col. 7, lines 7-28).

In claim 24, Nambu discloses the method of claim 14, wherein informing the sender comprises utilizing a public authenticated channel by the receiver to inform the sender (col. 1, lines 14-48; col. 4, line 63 – col. 5, line 53).

In claim 25, Nambu discloses the method of claim 14, wherein the channel parameters include an error rate and a line attenuation (col. 2, lines 10-57; col. 4, lines 4-42; col. 7, lines 7-49).

In claim 26, Nambu discloses the device of claim 17, additional comprising:

means for selecting, at a the emitter, two random numbers x_A and p_A from a Gaussian distribution of mean zero and variance V_AN_0, where N_0 refers to the shot-noise variance (col. 9, line 60 – col. 11, line 12);

means for sending a corresponding coherent state $|x_A + ip_A >$ in the quantum channel (col. 4, line 63 – col. 5, line 53);

means for randomly choosing, at the receiver, to measure either quadrature x or p using homodyne detection (col. 4, line 63 – col. 5, line 53; col. 6, line 34 – col. 7, line 6; col. 9, lines 36-59);

means for informing the emitter about the quadrature that was measured so the emitter may discard the wrong one (col. 2, lines 32-57);

means for measuring channel parameters on a random subset of the emitter's and receiver's data, in order to evaluate the maximum information acquired by an eavesdropper (col. 2, lines 32-57; col. 4, lines 4-42); and

means for converting the resulting raw key in the form of a set of correlated Gaussian variables into a binary secret key comprising direct or reverse reconciliation in order to correct the errors and get a binary key, and privacy amplification in order to make secret the binary key (col. 2, lines 32-57; col. 4, lines 4-42; col. 9, line 60 – col. 11, line 12).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Bennett, US 5,307,410; Bennett et al., US 5,515,438; Townsend, US 5,675,648; Townsend et al., 5,768,378; Townsend, US 5,953,421; Townsend, US 6,529,601; Blow, US 5,757,912; Phoenix et al., US 5,764,765; Brandt et al., US 5,999,285; Mazourenko et al., US 6,272,224; Patterson et al., US 6,289,104; Gisin et al., US 6,438,234; Wang, US 6,522,749; Mayers et al., US 6,678,379; Lehureau, US 6,778,669; Parks et al., US 2002/0041687; Azuma et al., US 2002/0106084; Nambu et al., US 2003/0002674.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JL

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137